Cyber Claims Examples

Social Engineering, Phishing, Phreaking and Cyber Fraud

Media Company

- 25 staff
- HKD50M turnover

Background

A hacker impersonated a client of the Insured, using an identical email address. The hacker emailed the Insured advising that future payments should be made to a new bank account. When the Insured was due to pay the client, they paid HKD205,000 into the fraudulent account.

Outcome

Indemnity was granted for the direct financial loss suffered by the Insured

Payment: HKD205,000.

Non for Profit

- 15 staff
- HKD2M turnover

Background

The Insured engaged a third party supplier for assistance in marketing their organisation and gathering donor's information; including names, emails and phone numbers. The Insured was advised that the third party supplier's system was breached and data had been lost.

Outcome

The Insured notified DUAL who appointed a law firm to advise in relation to the Insured's privacy legislation obligations. The Insured did not have to report the incident to the Privacy Commissioner based on individual circumstances and the IT data they had available to them. Payment was made in relation to the legal costs.

Payment: HKD29,500.

Hairdresser

- 5 staff
- HKD3M turnover

Background

The Insured uses a VoIP telephone system. A hacker gained access to the telephone system and made multiple unauthorised calls to a premium number over the course of a month. At the end of the month the Insured received their invoice, which included HKD150,000 of unauthorised calls.

Outcome

The client was covered for their direct financial loss as a result of the phreaking attack.

Payment: HKD150,000.

Insured by: MSIG

DUAL ASIA
Tel: +852 2530 6800 www.dualasia.com
Suite 2103, 21/F, Fu Fai Commercial Centre, 27 Hillier Street, Sheung Wan, Hong Kong
DUAL Underwriting Agency (Hong Kong) Limited - Licence number: FA2113

Accountant

- 6 staff
- HKD14M turnover

Background

The Insured's director noticed that some documents on their server had been deleted. Further investigations were undertaken and it was discovered a hacker had been accessing the Insured's system for the past 2 months.

Outcome

The Insured notified DUAL who hired an IT Forensic Consultant to review the Insured's systems. It was discovered 800 client files had been accessed which included private details such as driver's licenses and passport numbers. DUAL appointed a specialist firm to monitor whether any client identities were stolen or sold as well as a law firm to advise on the data breach issues and draft a notification letter to all affected parties. It was determined that the Insured had to report the incident to the Privacy Commissioner and the appropriate steps were taken to secure the information they held. Remediation costs were also covered to rectify any issues with the Insured's system.

Payment: HKD450,000.

Real Estate Agent

- 15 staff
- HKD10M turnover

Background

The Insured's emails were accessed by a hacker who posed as the Insured and sent multiple emails to the Insured's bank instructing for funds to be transferred into the hackers bank account. When the Insured discovered that 3 unauthorised payments had been made totaling HKD15,000,000 they immediately contacted their bank to freeze the funds. The Insured was able to recover HKD14,000,000 of the unauthorised transactions.

Outcome

The Insured notified DUAL who appointed Lawyers and an IT Forensic Consultant to assist the Insured in repairing the damage to their system which was caused by the hacker. As the Insured had Social Engineering cover under their policy, they were reimbursed for the direct financial loss of the HKD1,000,000 unrecovered fraudulent transfers as well as their forensic and legal costs.

Payment: HKD1,150,000.

Hotel Chain

- 50 staff
- HKD45M turnover

Background

The Insured hired a contractor to perform works on one of their properties. The Insured received an invoice for HKD65,000 from the contractor. The following week the Insured received an email claiming to be the contractor, stating that their bank details had changed and provided the new details. The Insured subsequently paid the HKD65,000 into the 'new' bank account. A few days later the contractor followed up the Insured for payment for their works at which time it was identified that their emails had been compromised and the Insured had paid a fraudulent account.

Outcome

The Insured was reimbursed for the direct financial loss suffered as a result of the fraud and additional costs payable under the policy.

Payment: HKD150,000.

Property Developer

- 7 staff
- HKD50M turnover

Background

Following the sale of 2 properties, the Insured was required to make a payment of HKD2,000,000 to their property consultant. On the day the payment was due, the Insured received an email from the consultant advising their banking details had changed. The Insured requested that this be sent to them in writing on the consultant's letterhead which they received, including the signature of the director of the consultancy company. The Insured was later chased by the consultant for payment at which time it was discovered that the email and letter had been fraudulent. The Insured contacted their bank to stop the payment and were informed that the money had already been withdrawn and transferred overseas.

Outcome

DUAL appointed an IT forensic consultant who identified that the hacker had infiltrated the consultants system and intercepted correspondence between the Insured and the consultancy firm. The Insured was reimbursed for the outstanding funds (capped at the Social Engineering sub limit of HKD1,250,000).

Payment: HKD1,250,000.